BÁO CÁO BÀI THỰC HÀNH SỐ 3

PHÂN TÍCH MỘT SỐ KỸ THUẬT TẤN CÔNG GIAO THỨC DNS

***Sinh viên 1: MSSV:***

***Sinh viên 2: MSSV:***

***Sinh viên 3: MSSV:***

***Yêu cầu kết quả thực hành:***

Đóng gói các kết quả vào file nén có tên theo định dạng NhomX\_Lab03\_BaoCao.zip

* Báo cáo kết quả thực hành
* File bắt lưu lượng đã yêu cầu. **Nếu không có đầy đủ file lưu lượng của kịch bản nào thì điểm của kịch bản đó là 0 điểm.**

**KẾT QUẢ THỰC HÀNH**

**Tạo thông điệp truy vấn DNS Query**

1. **Triển khai hệ thống (1 điểm)**

* Kết quả thực hiện lệnh tìm kiếm tên miền **# dig ns.attacker32.com**

*<Ảnh chụp kết quả>*

* Kết quả thực hiện lệnh tìm kiếm tên miền **# dig** [**www.example.com**](http://www.example.com)

*<Ảnh chụp kết quả>*

* Kết quả thực hiện lệnh tìm kiếm tên miền **# dig @ns.attacker32.com** [**www.example.com**](http://www.example.com)

*<Ảnh chụp kết quả>*

1. **Tạo thông điệp DNS Query truy vấn (2 điểm)**

Các thông tin trên thông điệp truy vấn đã sử dụng là gì? ***(1 điểm)***

* Địa chỉ IP nguồn:
* Số hiệu cổng nguồn:
* Địa chỉ IP đích:
* Số hiệu cổng đích:
* Tên miền được truy vấn:…… Tại sao thực hiện truy vấn tới một tên miền không tồn tại?***(1 điểm)***

1. **Tạo thông điệp DNS Response giả mạo (2 điểm)**

* Thông điệp DNS Response giả mạo gửi đi từ nút mạng nào? ***(0.5 điểm)***
* Các thông tin trên thông điệp trả lời giả mạo là gì? ***(1 điểm)***
* Địa chỉ IP nguồn
* Số hiệu cổng nguồn
* Địa chỉ IP đích
* Số hiệu cổng đích
* Thông tin tên miền đã giả mạo
* Để tấn công thành công, thì thông điệp trả lời giả mạo phải thỏa mãn các điều kiện gì?***(0.5 điểm)***

1. **Thực hiện tấn công (4 điểm)**

* Phân tích lưu lượng tấn công đã bắt được và chỉ ra thông điệp DNS Query mà Attacker đã gửi đi.***(0.5 điểm)***

*<Ảnh chụp gói tin trên Wireshark có các thông tin phù hợp ở mục 2>*

* Phân tích lưu lượng đã bắt được trên máy Local DNS Server và chỉ ra thông điệp DNS Query mà máy này đã gửi đi. Thông điệp này gửi tới máy nào? ***(0.5 điểm)***

*<Ảnh chụp gói tin trên Wireshark có các thông tin minh chứng>*

* Đặc điểm lưu lượng trên máy Local DNS Server khi bị tấn công là gì? ***(0.5 điểm)***

*<Ảnh chụp Wireshark để minh chứng>*

* Tìm ra gói tin DNS Response giả mạo đã được Local DNS Server chấp nhận. Tại sao khẳng định được gói tin này được Local DNS Server chấp nhận? ***(0.5 điểm)***

*<Ảnh chụp gói tin trên Wireshark có các thông tin minh chứng>*

* Phân tích nội dung bộ đệm dịch vụ của Local DNS Server để cho thấy tấn công đã thành công. ***(0.5 điểm)***

*<Ảnh chụp chỉ ra nội dung của bộ đệm dịch vụ trên Local DNS Server để minh chứng>*

* Phân tích kết quả tìm kiếm thông tin tên miền trên máy User để cho thấy Local DNS Server đã bị đầu độc. ***(0.5 điểm)***

*<Ảnh chụp kết quả của lệnh dig để minh chứng>*

* Từ các phân tích trên, mô tả một cách ngắn gọn kịch bản tấn công đã xảy ra.***(0.5 điểm)***
* Giải thích ngắn gọn và khái quát các hậu quả của cuộc tấn công? ***(0.5 điểm)***

1. **Phòng chống tấn công (1 điểm)**

Tại sao sử dụng cổng ứng dụng ngẫu nhiên để gửi thông điệp truy vấn DNS Query lại có tác dụng phòng chống tấn công DNS Cache Poisoning.